     Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   The Session Initiation Protocol (SIP) allows for users to make
   anonymous calls. However, users receiving such calls have the right
   to reject them because they are anonymous. SIP has no way to
   indicate to the caller that the reason for call rejection was that
   the call was anonymous. Such an indication is useful to allow the
   call to be retried without anonymity. This specification defines a
   new SIP response code for this purpose.

Table of Contents

1. Introduction

   The Session Initiation Protocol (SIP) [RFC3261] allows for users to
   make anonymous calls. In RFC 3261, this is done by including a From
   header field whose display name has the value of "Anonymous".
   Greater levels of anonymity were subsequently defined in [RFC3323],
   which introduces the Privacy header field. The Privacy header field
   allows a requesting User Agent (UA) to ask for various levels of
   anonymity, including user level anonymity, header level anonymity,
   and session level anonymity. [RFC3325] additionally defined the
   P-Asserted-Identity header field, used to contain an asserted
   identity. RFC 3325 also defined the 'id' value for the Privacy
   header field, which is used to request the network to remove the
   P-Asserted-Identity header field.

   Though users need to be able to make anonymous calls, users that
   receive such calls retain the right to reject the call because it is
   anonymous. SIP does not provide a response code that allows the User
   Agent Server (UAS), or a proxy acting on its behalf, to explicitly
   indicate that the request was rejected because it was anonymous. The
   closest response code is 403 (Forbidden), which doesn't convey a
   specific reason. While it is possible to include a reason phrase in
   a 403 response that indicates to the human user that the call was
   rejected because it was anonymous, that reason phrase is not useful
   for automata and cannot be interpreted by callers that speak a
   different language. An indication that can be understood by an
   automaton would allow for programmatic handling, including user
   interface prompts, or conversion to equivalent error codes in the
   Public Switched Telephone Network (PSTN) when the client is a
   gateway.

   To remedy this, this specification defines the 433 (Anonymity
   Disallowed) response code.

2. Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in [RFC2119].

3. Server Behavior

   A server (generally acting on behalf of the called party, though this
   need not be the case) MAY generate a 433 (Anonymity Disallowed)
   response when it receives an anonymous request, and the server
   refuses to fulfill the request because the requestor is anonymous. A
   request SHOULD be considered anonymous when the identity of the
   originator of the request has been explicitly withheld by the
   originator. This occurs in any one of the following cases:

   o The From header field contains a URI within the anonymous.invalid
      domain.

   o The From header field contains a display name whose value is
      either 'Anonymous' or 'anonymous'. Note that display names make a
      poor choice for indicating anonymity, since they are meant to be
      consumed by humans, not automata. Thus, language variations and
      even misspelling can cause an automaton to miss a hint in the
      display name. Despite these problems, a check on the display name
      is included here because RFC 3261 explicitly calls out the usage
      of the display name as a way to declare anonymity.

   o The request contained a Privacy header field whose value indicates
      that the user wishes its identity withheld. Values meeting this
      criteria are 'id' [RFC3325] or 'user'.

   o The From header field contains a URI that has an explicit
      indication that it is anonymous. One such example of a mechanism
      that would meet this criteria is [coexistence]. This criteria is
      true even if the request has a validated Identity header field
      [RFC4474], which can be used in concert with anonymized From
      header fields.

   Lack of a network-asserted identity (such as the P-Asserted-Identity
   header field), in and of itself, SHOULD NOT be considered an
   indication of anonymity. Even though a Privacy header field value of
   'id' will cause the removal of a network-asserted identity, there is
   no way to differentiate this case from one in which a network-
   asserted identity was not supported by the originating domain. As a
   consequence, a request without a network-asserted identity is
   considered anonymous only when there is some other indication of
   this, such as a From header field with a display name of 'Anonymous'.

   In addition, requests where the identity of the requestor cannot be
   determined or validated, but it is not a consequence of an explicit
   action on the part of the requestor, are not considered anonymous.
   For example, if a request contains a non-anonymous From header field,
   along with the Identity and Identity-Info header fields [RFC4474],

but the certificate could not be obtained from the reference in the
Identity-Info header field, it is not considered an anonymous
request, and the 433 response code SHOULD NOT be used.

4. UAC Behavior

   A User Agent Client (UAC) receiving a 433 (Anonymity Disallowed) MUST
   NOT retry the request without anonymity unless it obtains
   confirmation from the user that this is desirable. Such confirmation
   could be obtained through the user interface, or by accessing user-
   defined policy. If the user has indicated that this is desirable,
   the UAC MAY retry the request without requesting anonymity. Note
   that if the UAC were to automatically retry the request without
   anonymity in the absence of an indication from the user that this
   treatment is desirable, then the user's expectations would not be
   met. Consequently, a user might think it had completed a call
   anonymously when it is not actually anonymous.

   Receipt of a 433 response to a mid-dialog request SHOULD NOT cause
   the dialog to terminate, and SHOULD NOT cause the specific usage of
   that dialog to terminate [RFC5057].

   A UAC that does not understand or care about the specific semantics
   of the 433 response will treat it as a 400 response.

5. 433 (Anonymity Disallowed) Definition

   This response indicates that the server refused to fulfill the
   request because the requestor was anonymous. Its default reason
   phrase is "Anonymity Disallowed".

6. IANA Considerations

   This section registers a new SIP response code according to the
   procedures of RFC 3261.

   RFC Number: RFC 5079

   Response Code Number: 433

   Default Reason Phrase: Anonymity Disallowed

7. Security Considerations

   The fact that a request was rejected because it was anonymous does
   reveal information about the called party -- that the called party
   does not accept anonymous calls. This information may or may not be
   sensitive. If it is, a UAS SHOULD reject the request with a 403
   instead.

   In the Public Switched Telephone Network (PSTN), the Anonymous Call
   Rejection (ACR) feature is commonly used to prevent unwanted calls
   from telemarketers (also known as spammers). Since telemarketers
   frequently withhold their identity, anonymous call rejection has the
   desired effect in many (but not all) cases. It is important to note
   that the response code described here is likely to be ineffective in
   blocking SIP-based spam. The reason is that a malicious caller can
   include a From header field and display name that is not anonymous,
   but is meaningless and invalid. Without a Privacy header field, such
   a request will not appear anonymous and thus not be blocked by an
   anonymity screening service. Dealing with SIP-based spam is not a
   simple problem. The reader is referred to [sipping-spam] for a
   discussion of the problem.

   When anonymity services are being provided as a consequence of an
   anonymizer function acting as a back-to-back user agent (B2BUA)
   [RFC3323], and the anonymizer receives a 433 response, the anonymizer
   MUST NOT retry the request without anonymization unless it has been
   explicitly configured by the user to do so. In essence, the same
   rules that apply to a UA in processing of a 433 response apply to a
   network-based anonymization function, and for the same reasons.

8. Acknowledgements

   This document was motivated based on the requirements in
   [tispan-req], and has benefited from the concepts in [hautakorpi].
   Thanks to Keith Drage, Paul Kyzivat, and John Elwell for their
   reviews of this document.

9. References

9.1. Normative References

   [RFC3261]   Rosenberg, J., Schulzrinne, H., Camarillo, G.,
                    Johnston, A., Peterson, J., Sparks, R., Handley, M.,
                    and E. Schooler, "SIP: Session Initiation Protocol",
                    RFC 3261, June 2002.

   [RFC3323]   Peterson, J., "A Privacy Mechanism for the Session
                    Initiation Protocol (SIP)", RFC 3323, November 2002.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                    Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC4474]   Peterson, J. and C. Jennings, "Enhancements for
                    Authenticated Identity Management in the Session
                    Initiation Protocol (SIP)", RFC 4474, August 2006.

9.2. Informative References

   [RFC3325]   Jennings, C., Peterson, J., and M. Watson, "Private
                    Extensions to the Session Initiation Protocol (SIP)
                    for Asserted Identity within Trusted Networks",
                    RFC 3325, November 2002.

   [coexistence]   Rosenberg, J., "Coexistence of P-Asserted-ID and SIP
                    Identity", Work in Progress, June 2006.

   [tispan-req]   Jesske, R., "Input Requirements for the Session
                    Initiation Protocol (SIP) in support for the
                    European Telecommunications Standards Institute",
                    Work in Progress, July 2007.

   [hautakorpi]   Hautakorpi, J. and G. Camarillo, "Extending the
                    Session Initiation Protocol Reason Header with
                    Warning Codes", Work in Progress, October 2005.

   [RFC5057]   Sparks, R., "Multiple Dialog Usages in the Session
                    Initiation Protocol", RFC in 5057, November 2007.

   [sipping-spam]   Jennings, C. and J. Rosenberg, "The Session
                    Initiation Protocol (SIP) and Spam", Work
                    in Progress, August 2007.

Author's Address

    Jonathan Rosenberg
    Cisco
    Edison, NJ
    US

    EMail: jdrosen@cisco.com
    URI: http://www.jdrosen.net

Full Copyright Statement

Intellectual Property